

REMARKS

This Amendment and Response to Final Office Action is being submitted in response to the final Office Action mailed November 11, 2008. Claims 1-21 are pending in the Application.

Claims 1-12, 15-16, and 19-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* (U.S. Pat. Pub. 20030186679) in view of Zuk *et al.* (U.S. Pat. Pub. 20030154399) and Campbell *et al.* (U.S. Pat. No. 6,893,850).

Claims 13-14 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* in view of Zuk *et al.* and Campbell *et al.* as applied to Claim 1, and further in view of Won *et al.* (U.S. Pat. No. 6,754,488).

Claims 17-18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Challener *et al.* in view of Zuk *et al.* and Campbell *et al.* as applied to Claim 1, and further in view of Ammon *et al.* (U.S. Pat. Pub. No. 2003017289).

Based upon the arguments presented herein, reconsideration of the Application is respectfully requested.

Examiner's Response to Arguments

At the outset, none of the references used by the Examiner teach a set of one or more wireless receivers on one or more wireless sensors and the corresponding dynamic operational and security assessments which require information from the native wireless protocol. Challener *et al.* only monitors two data points – AP address and RF signal strength. Zuk *et al.* only monitors data packets on a wired connection, i.e. not in the native wireless protocol. Accordingly, this combination fails to meet Applicant's claims.

Zuk *et al.* teaches wired sensors located on a wired network for packet inspection. These are not wireless sensors located in proximity to a wireless network to monitor the packets, strip overhead, and perform analysis. As such, the sensors in Zuk *et al.* do not have

visibility to the wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings. Applicant respectfully stresses to the Examiner that none of the references teach wireless sensors to read wireless local area network (WLAN)-related overhead and data. There is no way that Zuk *et al.* can teach this structure. Specifically, Examiner states that Zuk *et al.*'s MMIDP system does deal with the wireless network (Final OA, page 2). However, the MMIDP sensors do not monitor wireless frames transmitted on the wireless network. These MMIDP sensors are monitoring traffic on the wired network only. Granted, a wireless network can attach to the wired network in Zuk *et al.*, but the wired network has no idea of the wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings.

Zuk *et al.* only deals with wired-based intrusions through its MMIDP sensors. As clearly shown in FIG. 3 of Zuk *et al.* the MMIDP sensor 45c is located on the wired network and it connects to a base station 72 through a wired connection. The MMIDP sensors do not have wireless radios nor do they do any analysis on WLAN network overhead (e.g. IEEE 802.11) since this overhead is stripped off and not passed onto the wireless network (from the base station 72). For example referring to FIG. 3 of Zuk *et al.*, the users 73a, b transmit to the base station 72 using a wireless protocol presumably. Applicant's invention has wireless sensors monitoring this wireless transmission in the wireless protocol for the tracking criteria, i.e. applying the dynamic operational and security assessments. Zuk *et al.*, on the other hand, only sees this transmission after it has passed the base station 72 to the wired network (again, this is clearly shown in FIG. 3 of Zuk *et al.*). Accordingly, once the transmission enters the wired network from the base station 72, it loses its wireless overhead in favor of the wired protocol overhead. Applicant respectfully notes that the MMIDP sensor has no visibility to the wireless protocol used by the users 73a, b. For example, the MMIDP sensor has no idea of the wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings (as claimed for wireless policy). There is no teaching in Zuk *et al.* that the base station 72 copies this data and forwards it to the MMIDP sensor for wireless policy analysis. Additionally, Zuk *et al.* is defining the wireless network 70 as a cell phone based network, not a WLAN as described by Applicant.

Next, Examiner argues that *Zuk et al.* teaches wireless policy. Again, based on the discussion above, *Zuk et al.* does not have visibility of wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings (Final OA, pages 2-3). Applicant agrees that *Zuk et al.* teaches policy enforcement for wired networks. However, there is no possible way that *Zuk et al.* could teach wireless policy as claimed. Granted, the MMIDP sensors are placed at the gateway to the wireless network, but they are not on the wireless network nor do they have access to the wireless network in the native protocols of the wireless network. Instead, these sensors view wired traffic coming off the wireless network in the wired network format.

Further, Examiner is mistaken to equate the authentication and encryption of *Zuk et al.* (¶[0005]-[0008]) with the wireless policy of the present invention. Here, *Zuk et al.* is specifically describing wired authentication and encryption using VPNs, firewalls, IP level address filtering, etc. These are not the same thing as WLAN wireless authentication and encryption, such as WEP, WPA, WPA2, etc. The Examiner is mistaken to state that *Zuk et al.* does disclose wireless policy as recited in the claims (Final OA, page 3). There is absolutely no discussion of IEEE 802.11 related policies in *Zuk et al.*

Next, Examiner claims that any techniques applied to wired networks would be equally applicable to wireless networks (Final OA, page 4). Granted, *Zuk et al.* teach policy deviation analysis to wired networks. However, our policy deviation detection uses completely different parameters as claimed. The present invention is monitoring all traffic transmitted over the wireless network, *Zuk et al.* is just monitoring packets which pass over its connections. The present invention analyzes policy deviation based on a combination of wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings. *Zuk et al.* has no view of these settings. In fact, *Zuk et al.* could not tell you one of these parameters through its MMIDP sensor. *Challener et al.* is no help here either. *Challener et al.* specifically state that the workstation acting as a monitor provides only two data points – whether there is a rogue access point (i.e. AP address) and the signal strength of the rogue access point (*Challener et al.*, ¶[0026]).

Next, the Examiner contends that the Claims require a set of one or more policy settings, not all of the policy settings cumulatively (Final OA, page 4). Applicant respectfully points out that Zuk *et al.* has no wireless policy settings --- our claim specifically states wireless policy settings. As described here in detail, Zuk *et al.* does not deal with wireless authentication despite Examiner's assertion to the contrary. Wireless authentication does not use VPNs, firewalls, etc. as taught by Zuk *et al.* Accordingly, Zuk *et al.* and any of the other references fail to teach this limitation:

wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings

Applicant can look at amending this limitation to recite three or more of the policy settings presuming that Examiner is claiming Zuk *et al.* teaches the authentication and encryption settings. However, Applicant respectfully stresses to Examiner that Zuk *et al.* teach none of these settings currently. Alternatively, Applicant can amend this limitation to recite wireless authentication settings and wireless encryption settings.

In the final paragraph on page 4 of the Final OA, Examiner rejects Applicant's argument that Zuk *et al.* fail to teach wireless statistics. Again, Applicant point out that Zuk *et al.* does not have visibility to the wireless protocol, so how can Zuk *et al.* gather wireless statistics? How many times the same IP address contacts during a given time period, etc. is not a wireless statistic, rather this is a layer three statistic or a wired statistic. Applicant goes through great detail in the Specification of describing the various monitored wireless statistics related to WLAN activity. IP address is a layer three protocol, not a layer two protocol or a WLAN wireless protocol.

On page 5 of the Final OA, the Examiner again states that the MMIDP sensors can view wireless traffic since they are at the gateway points of a wireless network. Applicant still points out that our claims as recited perform intrusion detection on wireless frames – our

sensors are distributed on the wireless network, not at a gateway on the wired network. The MMIDP sensors are performing intrusion detection on wired frames that have been adapted from a wireless protocol to a wired protocol. Thus the wired frames cannot be tested through wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests. These wired frames have no visibility into any of the wireless signatures, protocols, statistics, and policy.

Also, the Examiner argues that various arguments are not recited in the claims, such as stripping off wireless header information for wireless packets for gathering statistics, storing and processing wireless header information, etc. Applicant respectfully disagrees. From Claim 1, Applicants claim one or more wireless sensors and the steps of identifying a wireless device, receiving data from the one or more sensors, and storing the data:

- (a) identifying a wireless device for tracking based upon a combination of dynamic operational and security assessments derived using data from the system data store, wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device, wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings, and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings;

- (b) receiving data from a subset of the one or more wireless sensors;

- (c) storing the received data in the system data store, wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments, wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior;

Applicant respectfully notes that it is clear that the wireless sensors are monitoring the wireless header information. If required, Applicant can amend the claims to highlight these limitations.

Next, Examiner argues that Zuk *et al.* detects anomalous behavior because it updates a signature specific count of how many different hosts were contacted from the same IP address. Again, contacts from an IP address are not wireless statistics. Applicant goes through great detail in the specification describing the various wireless statistics and thresholds used. IP addresses are not one of them.

Finally, Examiner argues that the cited references disclose all of the structural limitations. Examiner is using Challener *et al.* to teach the set of one or more wireless receivers on one or more wireless sensors arguing that workstations and wireless access points configured to act as monitoring stations reads on wireless sensors as claimed by Applicants (Final OA, page 9). Applicant respectfully disagrees. Applicant's sensor devices as described in the specification differ significantly from a workstation with a wireless NIC card (as described in Challener *et al.*). Challener *et al.* specifically state that the workstation acting as a monitor provides only two data points – whether there is a rogue access point and the signal strength of the rogue access point (Challener *et al.*, ¶[0026]). Thus, there is no teaching on one or more wireless sensors. Zuk *et al.* and Challener *et al.* do not have access to the wireless packet overhead information to perform various intrusion detection analysis. Challener *et al.* is only looking at whether an AP is rogue or not (by looking at the MAC address versus an authorized AP list) and the RF signal strength. Zuk *et al.* is only looking at wired packets. Again, if required, Applicants can amend the claims to further highlight the functionality of the wireless sensors.

CONCLUSION

Applicant would like to thank Examiner for the attention and consideration accorded the present Application. Should Examiner determine that any further action is necessary to place the Application in condition for allowance, Examiner is encouraged to contact undersigned Counsel at the telephone number, facsimile number, address, or email address provided below. It is not believed that any fees for additional claims, extensions of time, or the like are required beyond those that may otherwise be indicated in the documents accompanying this paper. However, if such additional fees are required, Examiner is encouraged to notify undersigned Counsel at Examiner's earliest convenience.

Respectfully submitted,

Date: January 20, 2009

/ Lawrence A. Baratta Jr./

Lawrence A. Baratta Jr.

Registration No.: 59,553

Christopher L. Bernard

Registration No.: 48,234

Attorneys for Applicants

Clements | Bernard | Miller

1901 Roxborough Road, Suite 300

Charlotte, North Carolina 28211 USA

Telephone: 704.366.6642

Facsimile: 704.366.9744

lbaratta@worldpatents.com